ERIC A. GROVER (SBN 136080)
eagrover@kellergrover.com
ALEXANDER S. VAHDAT (SBN 284963)
avahdat@kellergrover.com
KELLER GROVER LLP
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861

Attorneys for Plaintiffs
BRIAN GRADY and MARK KLEIMAN

UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF CALIFORNIA

BRIAN GRADY and MARK KLEIMAN, on behalf of themselves and all other similarly situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC. and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC. Defendants.	Case No: **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Plaintiffs Brian Grady and Mark Kleiman ("Plaintiffs"), on behalf of themselves and all others similarly situated, file this Class Action Complaint ("Complaint") against Defendants Marriott International Inc. and Starwood Hotels & Resorts Worldwide, LLC (collectively "Marriott" or "Defendants"), and hereby allege the following:

NATURE OF THE ACTION

1. This class action seeks to redress Marriott's unlawful and negligent disclosure of millions of consumers' confidential personal identifying information ("PII"), including their names, addresses, email addresses, telephone numbers, dates of birth, gender, passport details, travel schedules, and credit card information in violation of California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (the "CLRA"), Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (the "UCL"), Customer Records Act, Cal. Civ. Code §§ 1798.80 *et. seq.* (the "CRA"), and common law claims for negligence and invasion of privacy.

2. Defendants have failed to fulfill their legal duty to protect consumers' PII which was stored in their systems. Defendants willful, reckless, and negligent disregard for their obligations to safeguard individuals' PII has resulted in a massive data breach that has been occurring since at least 2014, exposing hundreds of millions of consumers' PII ("Data Breach").

3. Plaintiff brings this action on behalf all California residents and other persons who reside in the United States whose PII was compromised as a result of the Data Breach (the "Classes" or "Class Members").

JURISDICTION, VENUE and PARTIES

4. This Court has subject matter jurisdiction over Plaintiffs claims pursuant to 28 U.S.C. § 1332(d) (CAFA) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5 million, exclusive of interest and costs.

5. This Court has personal jurisdiction over Defendants because both intentionally avail themselves of the rights and privileges of conducting business in California and have continuously and systematically had business contacts with California. Defendants own and/or operate multiple business locations in California, including in this judicial district.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

6. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims alleged by Plaintiffs occurred in this District.

7. Plaintiff Brian Grady is a citizen of California, and at all times relevant hereto was and is a resident of San Francisco, California. Since 2014, Mr. Grady has made numerous reservations for Starwood-branded properties while physically located within this judicial district and has stayed at various Starwood-branded properties since 2014, including Aloft BWI Airport, Westin Washington DC City Center, Aloft Bogota, The Prince Gallery Tokyo Kioicho, a Luxury Collection Hotel, and the W Hotel, Hong Kong.

8. Plaintiff Mark Kleiman is a citizen of California, and at all times relevant hereto was and is a resident of Los Angeles, California. Mr. Kleiman made a reservation and stayed at a Starwood-branded property at least once since 2014, including his October 2014 stay at Aloft in Brooklyn, New York.

9. Defendant Marriott International, Inc. is incorporated under the laws of the State of Delaware, with its principal place of business in Bethesda, Maryland. Marriott operates through various subsidiaries, each of which acts as an agent of or in concert with Defendant Marriott International, Inc.

10. Defendant Starwood Hotels & Resorts Worldwide, LLC is incorporated under the laws of the State of Maryland, with its principal place of business in Bethesda, Maryland.

FACTUAL ALLEGATIONS

A. THE MARRIOTT DATA BREACH

11. Marriott owns and operates a variety of hotel, lodging, and hospitality brands, including hotels under its Starwood brands, which include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels. Hundreds of millions of customers have made reservations and stayed at Starwood properties around the globe.

12. Since at least 2014, when booking reservations at a Starwood property,

customers have and do provide Defendants with sensitive PII, including their names, addresses, passport numbers and details, phone numbers, email addresses, dates of birth, gender, travel schedules, and credit card numbers with expiration dates.

13. Individuals who entrust Defendants with PII, which includes extremely sensitive data such as passport details and credit card information, do so with the understanding that Defendants will safeguard that information. That expectation is directly reinforced by Marriott, which publicly touts its commitment to safeguarding customers PII. For example, in its Marriott Group Global Privacy Statement, Marriott purports to "use reasonable organizational, technical and administrative measures to protect Personal Data."[1] Likewise, Defendants' Marriott U.S. Privacy Shield Guest Privacy Policy represents to customers that it will "use reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction."[2]

14. Despite these promises to safeguard guests' PII, in a November 30, 2018 statement, Marriott revealed that data for approximately 500 million guests was exposed in an ongoing hack that has allowed unauthorized access to its Starwood Hotels reservation database since 2014, and that hackers have actively copied and encrypted information from this database.[3] The statement further revealed that Defendant initially discovered the Data Breach months earlier, on September 8, 2018.[4]

15. The Data Breach compromised "some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences" for at least 327 million individuals, and names, mailing addresses and unidentified "other information" for at least 150 million other individuals.[5]

---

[1] *See* https://www.marriott.com/about/privacy.mi (last accessed Nov. 30, 2018).
[2] *See* https://www.marriott.com/about/global-privacy.mi (last accessed Nov. 30, 2018).
[3] *See Marriott Announces Starwood Guest Reservation Database Security Incident*, MARRIOTT NEWS CENTER (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).
[4] *See id.*
[5] *See id.*

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

16. At this time, it is unclear why the Data Breach was not discovered over the past four years, or why it took over two-and-a-half months for Marriott to verify and report the Data Breach to the victims whose PII had been stolen. Such a delay is damaging to the Data Breach's victims, in that they could have immediately acted in a manner to protect themselves and their PII from further harm.

B. DATA BREACHES RESULT IN IDENTITY THEFT

17. Data thieves intentionally hack into inadequately protected servers to steal PII with the primary incentive of weaponizing that private data to commit identity theft and financial fraud. Identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.

18. Given the scope of this Data Breach and the nature of the PII compromised, the ways in which criminals may unlawfully use the data is limitless, as is the timeframe for using the information for criminal endeavors.

19. Unfortunately for Plaintiff and the Class, a person whose PII has been compromised may not fully experience the effects of the breach for years to come.

20. The information implicated in this Data Breach is particularly susceptible to criminal activity. According to experts, information such as a history of home addresses and travel destinations gives hackers additional information to crack security questions. Detailed personal information also allows criminals to design and execute more sophisticated phishing scams.

21. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[6]

[6] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

22. As a direct and proximate result of Marriott's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII, Plaintiff and the Class are susceptible to identity theft.

23. The risks associated with identity theft are serious. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, banking or finance fraud, and government fraud. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[7]

24. Having obtained the Plaintiff and Class Members' names, addresses, passport details, phone numbers, email addresses, dates of birth, gender, and credit card numbers and expiration dates, cybercriminals can simply use the data revealed or pair the data with other available information to commit a broad range of fraud in a victim's name.

25. Passport data was also included in the breach. Having obtained the Plaintiff and Class Members' passports, cybercriminals can use the data to commit a broad range of fraud in a victim's name, including opening bank accounts, and illegally entering the country and masking their identity from the authorities.[8]

26. Beyond using the data exposed for nefarious purposes themselves, the cybercriminals who obtained Plaintiff and Class Members' PII may also exploit the data by selling it on the "black market" or "dark market" for years following a breach. There is a well-established international black market where hackers may quickly and efficiently sell -- in part or in whole -- precisely the type of PII stolen in the instant Data Breach.

---

[7] True Identity Protection: Identity Theft Overview, http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf (visited Sept. 23, 2016).

[8] Gabriel Wood, *Common Forms of ID Criminal Use to Commit Identity Theft, available at* https://www.nextadvisor.com/blog/common-forms-of-id-criminals-use-to-commit-identity-theft/

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

27. The PII exposed in the Breach, which included, *inter alia*, names, birth dates, and addresses qualifies as what hackers and black markets term as "fullz" records.[9] According to one 2015 estimate, the median price for someone's identity on the black market is approximately $21.35.[10] Fullz records are notably on the higher end of the pricing spectrum because they entail a "full set" of individuals' PII and the range of PII sold in the same markets also includes less glamorous information, such as basic credit card information.

28. Cybercriminals can further post stolen PII on the internet, thereby making such information publicly available.

29. Individuals whose PII is subject to a reported security breach -- such as the Data Breach at issue here -- are approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft.[11]

C. MARRIOTT KNEW THE RISK OF CYBERSECURITY ATTACKS

30. Data security breaches -- and data security breach litigation – have dominated the headlines in recent years, including into 2018.[12] According to the Privacy Rights Clearinghouse Chronology of Data Breaches, over 1,300 breaches were publicly reported in 2017 and 2018 alone.[13]

---

[9] Brian Feldman, *So What Happens With All That Equifax Data?* N.Y. Magazine, Sept. 8, 2017, http://nymag.com/selectall/2017/09/so-what-happens-with-all-that-equifax-data.html.

[10] Keith Collins, *Here's what your stolen identity goes for on the internet's black market*, Quartz, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

[11] See Javelin Strategy & Research, *Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier, available at* https://www.javelinstrategy.com/news/1314/92/1 (last visited Jun. 16, 2014).

[12] *See e.g.*, Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN Tech (Sept. 23, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/; Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could Be Affected*, CNN Tech (Sept. 8, 2017), https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html; Jim Finkel and David Henry, *Saks, Lord & Taylor Hit By Payment Card Data Breach*, Reuters (Apr. 3, 2018), https://www.reuters.com/article/legal-us-hudson-s-bay-databreach/saks-lord-taylor-hit-by-payment-card-data-breach-idUSKCN1H91W7; Bill Hutchinson, *87 million Facebook Users To Find Out If Their Personal Data Was Breached*, ABC News (Apr. 9, 2018), https://abcnews.go.com/US/87-million-facebook-users-find-personal-data-breached/story?id=54334187.

[13] *See* Privacy Rights Clearinghouse Chronology of Breaches *available at* http://www.privacyrights.org.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

31. The hospitality industry has become a main target of cyber-attacks. Many other hospitality chains have had major PII breaches. Since the hospitality industry has become a target for attackers, Marriott was clearly aware of this threat.[14]

32. In SEC filings, Marriott recognized that its, "reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years."[15]

33. Moreover, this is not the first time Defendants have faced a data breach. Starwood properties was implicated in a 2016 data breach.[16]

D. PLAINTIFFS AND CLASS MEMBERS HAVE SUFFERED DAMAGES BECAUSE OF THE DATA BREACH

34. The Data Breach was a direct and proximate result of Defendants failure to properly safeguard and protect Plaintiffs and Class Members' PII against reasonably foreseeable threats to the security or integrity of such information.

35. Defendants failed to identify, implement, maintain, and monitor appropriate data security measures, policies, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiffs and Class Members' PII.

36. Defendants improperly handled Plaintiffs and Class Members' PII. Plaintiffs was improperly handled, stored, segregated, and in some cases, either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols. Indeed, Marriott itself conceded that only credit card

---

[14] See Hospitality Technology, *Cybersecurity Tactics for a Hotel Industry that's Under Siege*, *available at* https://hospitalitytech.com/cybersecurity-tactics-hotel-industry-thats-under-siege (last visited Nov. 30, 2018).

[15] Marriott International Inc., Annual Report (Form 10-K) (Feb. 15, 2018).

[16] Alwyn Scott, Starwood, *Marriott, Hyatt, IHG hit by malware: HEI*, REUTERS, Aug. 14, 2016, https://www.reuters.com/article/us-hotels-cyber/starwood-marriott-hyatt-ihg-hit-by-malware-hei-idUSKCN10P0ZM.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

data was encrypted.[17] Had Defendants taken appropriate security measures, the Data Breach would not have occurred.

37. The PII Defendants exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

38. Unfortunately for Plaintiffs and Class members, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

39. Accordingly, Plaintiffs and Class members will bear a heightened risk of injury for years to come. Identity theft is one such risk and occurs when an individuals' PII is used without his or her permission to commit fraud or other crimes.[19]

40. According to the Federal Trade Commission, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[20]

---

[17] *See Marriott Announces Starwood Guest Reservation Database Security Incident*, Marriott News Center (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last accessed Nov. 30, 2018).

[18] G.A.O., Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007) http://www.gao.gov/assets/270/262904.html [as of June 24, 2017].

[19] Fed. Trade Comm'n, Taking Charge: What to do if your identity is stolen (April 2013) https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf [as of June 24, 2017].

[20] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change (March 2012) https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-

41. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiffs' and Class members' PII, and Defendants' failure to properly and timely remediate the Data Breach and give Class members notice of the Data Breach, Plaintiffs and Class members are more susceptible to identity theft and have experienced, will continue to experience and will face an increased risk of experiencing the following injuries, *inter alia*:

- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

---

protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [as of June 24, 2017].

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Defendants fail to undertake appropriate, legally required steps to protect the personal information in its possession.

42. The risks associated with identity theft are serious. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[21]

43. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

CLASS ACTION ALLEGATIONS

44. Plaintiffs bring this action on their own behalf, and on behalf of all persons similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure. Plaintiffs seek to represent the following Nationwide Class:

> All persons who reside in the United States whose personally identifiable information was accessed, compromised, stolen or acquired by unauthorized persons as a result of the Data Breach.

[21] True Identity Protection: Identity Theft Overview, ID Watchdog http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf [as of Sept. 23, 2016].

45. Additionally, Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on their own behalf and on behalf of all persons similarly situated within the state of California (the "California Class"), defined as follows:

> All persons who reside in the State of California whose personally identifiable information was accessed, compromised, stolen or acquired by unauthorized persons as a result of the Data Breach.

46. Plaintiffs reserve the right to modify or amend the Class definitions before the Court determines whether class certification is appropriate.

47. The members of the Class are so numerous, numbering in the millions, such that their joinder is impracticable. Their identities and contact information can be easily derived from Defendants' internal records.

48. The rights of Plaintiffs, and each Class member, were violated in precisely the same manner by Defendants' reckless and negligent actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII.

49. There are questions of law and fact common to the Class as a whole. The common questions of law and fact predominate over any questions affecting only individual members of the Class, and include, without limitation:

a. Whether Defendants had a duty to protect Plaintiffs' and the Class members' PII;

b. Whether Defendants breached their duty to protect Plaintiffs' and the Class members' PII;

c. Whether Defendants' breach of a legal duty caused its systems to be compromised, resulting in the loss and/or potential loss of Plaintiffs and Class members users' PII;

d. Whether Defendants properly designed, adopted, implemented, controlled, managed and monitored data security processes, control, policies, procedures and/or protocols to protect Plaintiffs' and the Class members' PII in the Data Breach;

e. Whether Defendants timely and adequately investigated the Data Breach and took reasonable remedial actions in response to the Data Breach';

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

f. Whether Defendants failed to timely and adequately inform Plaintiffs and the Class members of the Data Breach;

g. Whether Defendants' conduct was negligent;

h. Whether Defendants' conduct was willful; and

i. Whether Plaintiffs and Class members are entitled to damages.

50. Plaintiffs' claims are typical of the claims of the Class members because Plaintiffs, like all Class members, are victims of Defendants wrongful actions, inaction, and omissions that caused the Data Breach, caused the unauthorized release and disclosure of their PII. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs' counsel is highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

51. The representative Plaintiffs will fairly and adequately represent the members of the Class and have no interests that are antagonistic to the claims of the Class. The Plaintiffs' interests in this action are antagonistic to the interests of Defendants, and Plaintiffs will vigorously pursue the claims of the Class.

52. The representative Plaintiffs have retained counsel who are competent and experienced in consumer, data breach, and invasion of privacy class action litigation, and have successfully represented plaintiffs in complex class actions. Plaintiffs' counsel currently represents other plaintiffs in similar complex class action litigation involving wrongful disclosures and access of private information.

53. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiffs and the Class are nearly identical and will require evidentiary proof of the same kind and application of the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

54. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class members number in the millions and individual joinder is impracticable. The expense and burden of individual litigation would make it

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

impracticable or impossible for proposed Class members to prosecute their claims individually. Trial of Plaintiffs' and the Class members' claims is manageable. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

55. The persons in the Class are so numerous that the joinder of all such persons individually in this case is impracticable, and the disposition of their claims in this case and as part of a single class action lawsuit, rather than hundreds or thousands of individual lawsuits, will benefit the parties and greatly reduce the aggregate judicial resources that would be spent if this matter were handled as hundreds or thousands of separate lawsuits.

56. Plaintiffs are not aware of any difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action.

57. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class Members.

FIRST CAUSE OF ACTION
(Violation of California Consumers Legal Remedies Act, California Civil Code § 1750 *et seq.*)

58. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

59. This cause of action is brought on behalf of the California Class pursuant to the California Consumers Legal Remedies Act ("CLRA"), California Civil Code § 1750, *et seq.* This cause of action does not seek monetary damages at this time and is limited solely to injunctive relief. Plaintiffs will later amend this class action Complaint to seek damages in accordance with the CLRA after providing Defendants with notice as required by Civil Code section 1782.

60. Plaintiffs and California Class members are "consumers," as the term is defined by California Civil Code section 1761, subdivision (d).

61. Plaintiffs, California Class members, and Defendants have engaged in "transactions," as that term is defined by Civil Code section 1761, subdivision (e).

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

62. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Defendants was likely to deceive consumers.

63. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

64. Defendants violated this provision by representing that they would take appropriate measures to protect Plaintiffs' and the California Class members' PII, take its customers' privacy seriously, limit access its customers' PII, and comply with the law. Defendants however improperly handled, stored, or protected either unencrypted or partially encrypted data consisting of its customers' PII. Defendants also failed to adequately notify its users of the Data Breach, instead choosing to hide such information in favor of its acquisition and profits, causing Plaintiffs additional harm.

65. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

66. Defendants violated this provision by representing that their data security would adequately protect its customers' personal information, and would not allow that information to be provided to any unauthorized parties.

67. Plaintiffs and the California Class members relied upon Defendants' representations and were induced to do make reservations to stay at Defendants' properties and provide their PII which contains value in order to obtain services from Defendants.

68. As a result of engaging in such conduct, Defendants have violated Civil Code section 1770.

69. Pursuant to Civil Code section 1780, subdivisions (a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law, and requiring Defendants to take remedial measures to ensure the Data

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

Breach and its improper business practices in monitoring, remediating and responding to the Data Breach will not happen again.

70. Plaintiffs and the California Class members suffered injuries caused by Defendants misrepresentations and omissions, because they provided their PII believing that Defendants would adequately protect this information.

71. Plaintiffs and the California Class members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

72. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiffs and members of the California Class.

SECOND CAUSE OF ACTION
(Violation of Unfair Competition Law California Business and Professional Code Sections 17200 *et seq.*)

73. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

74. Plaintiffs bring this claim on behalf of themselves and the California Class.

75. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

76. By reason of Defendants above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and California Class members' PII, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning of the UCL.

77. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous and substantially injurious to consumers, in that the private and confidential PII of Plaintiffs and the California Class members has been compromised for all to see, use, or otherwise exploit.

78. Defendants' practices were unlawful and in violation of Civil Code sections 1798 *et seq.* and Defendants' own privacy policy because Defendants failed to take reasonable measures to protect Plaintiffs' and the California Class members' PII and failed to take remedial

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

measures such as notifying its users when it first discovered that their PII may have been compromised.

79. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Defendants will remain private and secure, when in fact it was not private and secure, and that Defendants would take proper measures to investigate and remediate the Data Breach, when Defendants did not.

80. Plaintiffs and the California Class members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants above-described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII.

81. Defendants above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and California Class members' PII also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq*., in that Defendants' conduct was substantially injurious to Plaintiffs and California Class members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

82. But for Defendants misrepresentations and omissions, Plaintiffs and California Class members would not have provided their PII to Defendants, or would have insisted that their PII be more securely protected.

83. As a direct and proximate result of Defendants above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs and California Class members' PII, they have been injured as follows: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendants; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their PII; and (5) costs associated with monitoring their PII, amongst other things.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

84. Plaintiffs takes upon themselves enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiffs by forcing them to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under Code of Civil Procedure section 1021.5.

THIRD CAUSE OF ACTION
(Violation of California Customer Records Act,
Cal. Civ. Code §§ 1798.80 *et seq.*)

85. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

86. "[T]o ensure that personal information about California residents is protected," Civil Code section 1798.81.5 requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

87. Defendants own, maintain, and license personal information, within the meaning of section 1798.81.5, about Plaintiffs and the California Class.

88. Defendants violated Civil Code section 1798.81.5 by failing to implement reasonable measures to protect Plaintiffs' and Class members' personal information, to remediate the Data Breaches, and to timely and adequately notify California Class members.

89. As a direct and proximate result of Defendants violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred and harms stemming from the Data Breach were not timely cured.

90. In addition, California Civil Code section 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . .”

91. Section 1798.2(b) provides that “[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

92. Defendants are businesses that own or license computerized data that includes personal information as defined by Civil Code sections 1798.80 *et seq*.

93. In the alternative, Defendants maintain computerized data that includes personal information that Defendants does not own as defined by Civil Code sections 1798.80 *et seq*.

94. Plaintiffs’ and California Class members’ personally identifiable information (including but not limited to names, addresses, and passport information) includes personal information covered by Civil Code § 1798.81.5(d)(1).

95. Because Defendants reasonably believed that Plaintiffs’ and the California Class members’ personal information was acquired by unauthorized persons during the Data Breach, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Civil Code section 1798.82(a), or in the alternative, under Civil Code section 1798.82(b).

96. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Civil Code section 1798.82.

97. As a direct and proximate result of Defendants violations of Civil Code sections 1798.81.5 and 1798.82, Plaintiffs and California Class members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased imminent risk of fraud and identity theft, and loss of value of their personally identifying information.

98. Plaintiffs and California Class members seek relief under Civil Code section 1798.84 including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

///

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

FOURTH CAUSE OF ACTION
(Negligence)

99. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

100. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

101. Plaintiffs and Nationwide Class members were required to provide Defendants with certain PII in connection with their hotel reservations and stays. Defendants collected and stored this information including their names, addresses, credit card information and passport information.

102. Defendants had a duty to Plaintiffs and Nationwide Class members to safeguard and protect their PII, including the duty to timely and reasonably investigate and remediate the Data Breach and notify Nationwide Class members timely and adequately concerning the Data Breach.

103. Defendants assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, to detect any attempted or actual breach of its systems, to timely and reasonably investigate and remediate the Data Breach and to notify Nationwide Class members timely and adequately concerning the Data Breach.

104. Defendants had full knowledge about the sensitivity of Plaintiffs' and Nationwide Class members' PII, as well as the type of harm to could occur if such PII was wrongfully disclosed, if disclosure was not timely or adequately remediated, or if Nationwide Class members were not timely and adequately alerted to the Data Breach.

105. Defendants had a special relationship with Plaintiffs and Nationwide Class members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiffs' and Nationwide Class members' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, Defendants were capable of protecting their networks and systems, and the PII it stored on them, from unauthorized access, but failed to do so time and time again. Defendants repeated security incidents and its numerous acquisitions over many years

demonstrated to them that the harm to Plaintiffs and Nationwide Class members was foreseeable. The massive size and ongoing nature of the Data Breach, Defendants' failure to disclose the Data Breach to the public when they first discovered the intrusions, and their lack of remediation following the Data Breach demonstrate that Defendants are morally to blame for the Data Breach, and cannot be trusted to prevent future data breaches.

106. Defendants had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with customer PII data and data breaches.

107. Defendants breached their duty of care by failing to secure and safeguard the PII of Plaintiffs and Nationwide Class members, failing to timely and reasonably investigate and remediate the Data Breach and failing to timely and adequately inform Nationwide Class members concerning the Data Breach. Defendants negligently stored and/or maintained their systems.

108. Further, Defendants, by and through its above negligent actions and/or inaction, further breached their duties to Plaintiffs and Nationwide Class members by failing to design, adopt, implement, control, manage, monitor, remediate, investigate and audit its processes, controls, policies, procedures, vulnerabilities and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Nationwide Class members' PII within its possession, custody and control.

109. Plaintiffs and the other Nationwide Class members have suffered harm as a result of Defendants' negligence. Plaintiffs and Nationwide Class members' loss of control over their compromised PII has subjected and continues to subject each of them to harms stated herein, including but not limited to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, and access to their user accounts.

110. It was reasonably foreseeable—in that Defendants knew or should have known—that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Nationwide Class members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

wrongful use and for no lawful purpose. It was reasonably foreseeable—in that Defendants knew or should have known—that their failure to timely and reasonably investigate and remediate the Data Breach and to notify Class members in a timely and adequate manner concerning the Data Breach, would result in further release and disclosure of the information to unauthorized third parties, as well as further exposure to harms due to Nationwide Class members' delay in addressing and attempting to cure risks associated with identity theft and misuse of their information by third parties.

111. But for Defendants negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Nationwide Class members, their PII would not have been compromised and the harms alleged herein would not have been incurred.

112. As a direct and proximate result of Defendants above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Nationwide Class members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm—for which they are entitled to compensation. Defendants wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

113. Plaintiffs and Class members are entitled to injunctive relief as well as actual and punitive damages.

FIFTH CAUSE OF ACTION
(Invasion of Privacy)

114. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

115. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

116. Plaintiffs and Nationwide Class members have a legally protected privacy interest in their PII that Defendants required them to provide and stored.

117. Plaintiffs and Nationwide Class members reasonably expected that their PII would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861

118. Defendants unlawfully invaded the privacy rights of Plaintiffs and Nationwide Class members by (a) failing to adequately secure their PII from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII to unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII to unauthorized parties without the informed and clear consent of Plaintiffs and Nationwide Class members. Further, Defendants invaded the privacy rights of Plaintiffs and Nationwide Class members by failing to adequately or timely take steps to remediate the Data Breach, or provide Nationwide Class members notice of the Data Breach, once Defendants possessed knowledge to a substantial certainty that the Data Breach was occurring and that Nationwide Class members were being harmed. This invasion into the privacy interest of Plaintiffs and Nationwide Class members is serious and substantial.

119. In failing to adequately secure Plaintiffs' and Nationwide Class members' PII, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiffs and Nationwide Class members.

120. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiffs' and Nationwide Class members' PII has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiffs and the Nationwide Class have suffered injury as a result of Defendants unlawful invasions of privacy and are entitled to appropriate relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment as follows:

1. For an Order certifying the proposed Classes pursuant to FED. R. CIV. P. 23(b)(1), (2) and/or (3), appointing Plaintiffs as Class Representative for each Class, and appointing Eric A. Grover of Keller Grover LLP as Class Counsel;

2. For appropriate injunctive relief and/or declaratory relief, including, but not limited to, an order requiring Defendants to immediately secure and fully encrypt all confidential information, to cease negligently storing, handling, and securing

its users confidential information, to notify users whose PII is wrongly disclosed in an expedient and timely manner and to provide identity theft monitoring;

3. Adjudging and decreeing that Defendants have engaged in the conduct alleged herein;

4. For compensatory and general damages according to proof on certain causes of action;

5. For reimbursement, restitution and disgorgement on certain causes of action;

6. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

7. For costs of the proceedings herein;

8. For reasonable attorneys' fees as allowed by California Code of Civil Procedure Section 1021.5, and any other applicable statutes; and

9. For any and all such other and further relief that this Court may deem just and proper.

Respectfully submitted,

Dated: December 4, 2018

KELLER GROVER LLP

By: _____
ERIC A. GROVER
Attorneys for Plaintiff

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims and causes of action in this lawsuit to which they are so entitled.

Dated: December 4, 2018

KELLER GROVER LLP

By: _____
ERIC A. GROVER
Attorneys for Plaintiff

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax 415.543.7861